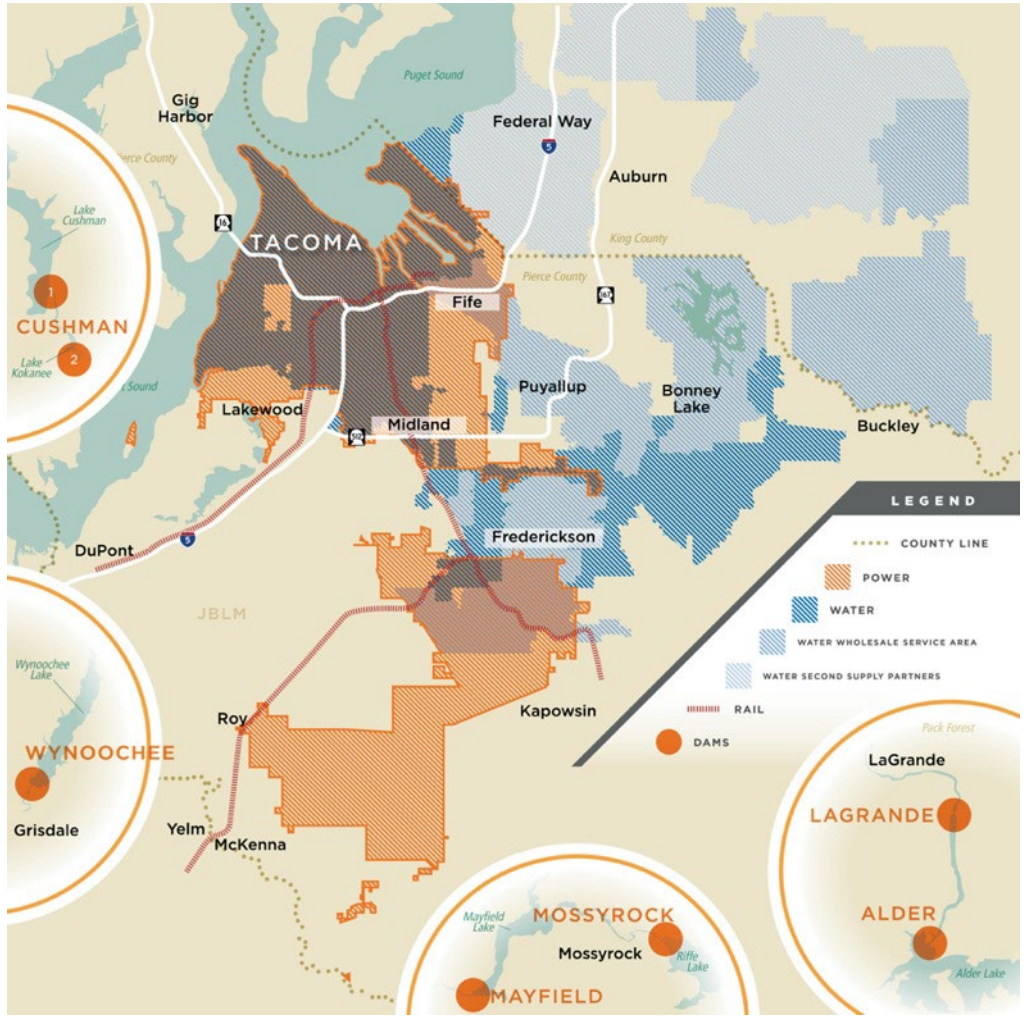
Cybersecurity Update

Nate Walters, Cybersecurity Operations Manager

TACOMA PUBLIC UTILITIES

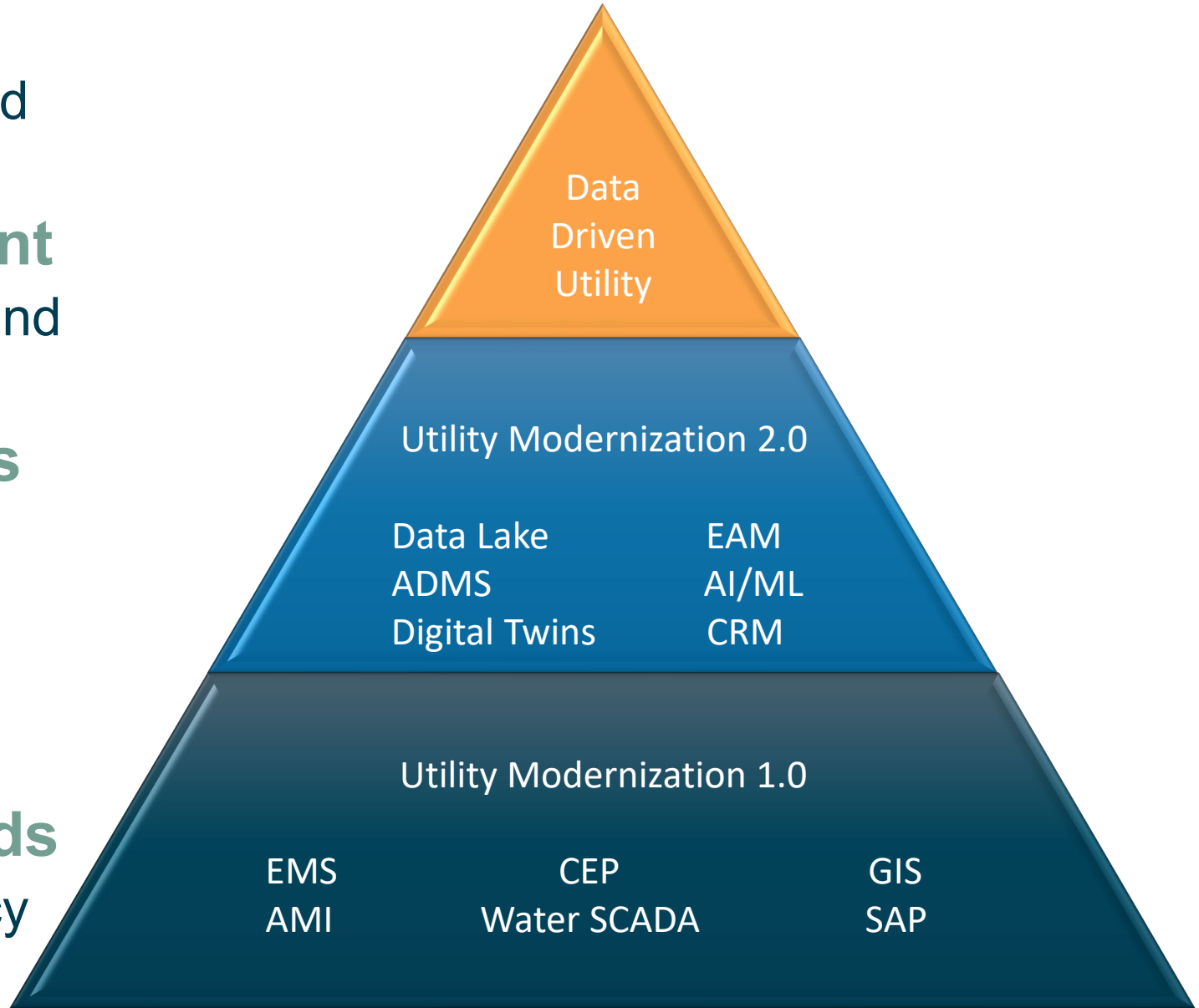
Agenda



- Supporting Utility Modernization
- New Requirement: CIP-015
- Threat Brief
- PUB training

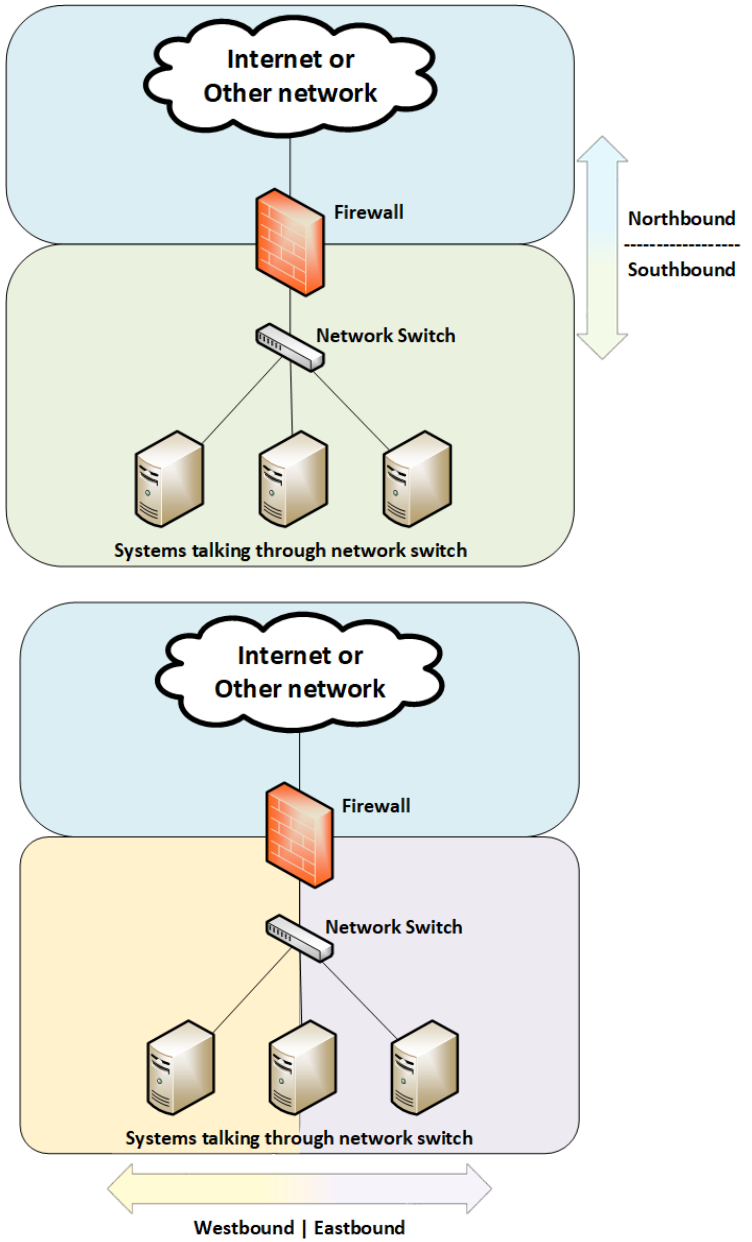
Supporting Utility Modernization

- **Operations**
  - Daily monitoring, triage, and response
- **Vulnerability Management**
  - Risk-based assessments and remediation
- **Security Design Reviews**
  - Ensuring industry best practices
- **Network Monitoring**
  - Driving visibility
- **Policies, Plans, Standards**
  - Foundation and consistency



New Requirement: CIP-015

- **New CIP-015 Requirement**
  - **Purpose**: “To improve the probability of detecting anomalous or unauthorized network activity in order to facilitate improved response and recovery from an attack.”
  - **Requires** TPU to *Monitor*, *Detect*, *Evaluate*, and *Retain* traffic between systems in our control centers.
  - **Complements** existing Intrusion Detection System
  - **Net new** cybersecurity capability
  - **Future versions** will increase scope



Threat Brief – Voltzite APT

VOLTZITE, an Advanced Persistent Threat group with operational overlaps with Volt Typhoon, is performing reconnaissance and enumeration of multiple US-based electric companies and has been observed targeting electric power transmission and distribution, emergency services, telecommunications, defense industrial bases, and satellite services.

CAPABILITIES

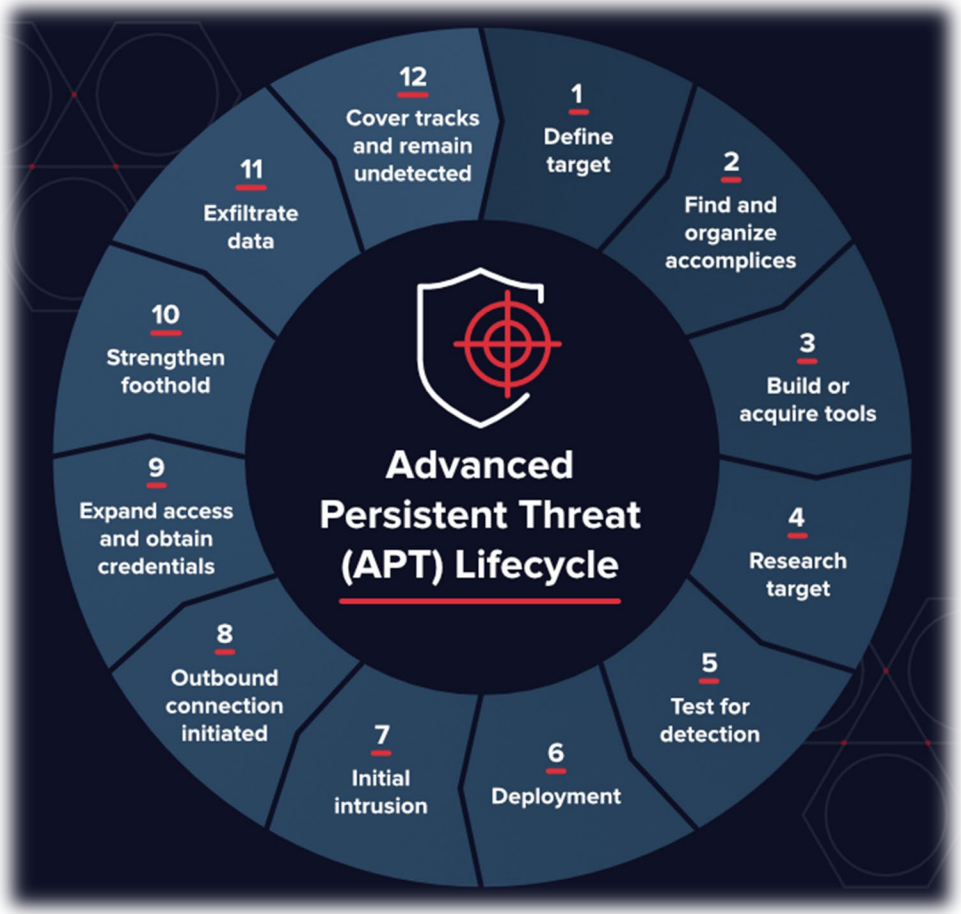
- Heavy use of living off the land techniques
- Slow steady reconnaissance to evade detection
- Focus on lateral movement between IT and OT

Targets

- Electric sector across the United States

IMPACT

- Loss of Confidentiality, Theft of Operational Information
- Espionage and persistent access
- Battlespace preparation for future conflicts



How We're Addressing these Threats

- **Detection and Response**
  - Network traffic inspection
  - Endpoint Detection and Response
  - Analysts monitoring and responding to alerts
  - Partnerships
- **Managing Vulnerabilities**
  - Vulnerability Management Program
  - External Attack Surface Monitoring
- **Design**
  - Network Segmentation
  - Security Design Reviews
- **Practice**
  - Cybersecurity Incident Response Exercises

PUB Training

- **Phishing Awareness**
  - AI tools are elevating phishing campaigns
  - Email, text, voice, video
- **Password Manager**
  - Remember one password, forget the rest
  - Unique passwords limit impact from compromise
- **Multi-Factor Authentication (MFA)**
  - Most impactful security control
  - Something you have + something you know
- **Personal Awareness and Action**
  - Monitor for compromise; act promptly
  - Keep devices updated

Questions & Feedback